CSS 11000 および CSS 11500 でのセキュリティの向上

目次

概要

このドキュメントでは、Cisco コンテンツ サービス スイッチ（CSS）11000 または CSS 11500 のセキュリティを向上できる Cisco コンフィギュレーション設定について説明します。 このドキュメントでは、IP ネットワークのほぼ全的に適用できる基本的なコンフィギュレーション設定について説明し、不測の事態を招くいくつかの要注意項目を取り上げています。

このドキュメントは、次の項目のすべてを網羅したリストではありません。また、このドキュメントの情報を、ネットワーク管理者の知識に代えて使用することもできません。 このドキュメントは、項目を憶えておくための助けとして機能します。

このドキュメントには、IP ネットワークの重要なコマンドだけが記載されています。 ユーザが CSS で有効化できるサービスの多くには、注意深いセキュリティ設定が必要です。 ただし、このドキュメントでは、デフォルトで有効であるか、ほとんどの場合はユーザが有効にし、無効化または再設定が必要になることのあるサービスの詳細について重点的に説明します。

Cisco WebNS ソフトウェアのデフォルト設定には、これまでの経緯により存在しているものがあります。 これらの設定は、選択された時点では適用可能でしたが、新しいデフォルトが現在選択されている場合には、状況が異なります。 その他のデフォルトは、ほとんどのシステムに適用できますが、ネットワークの境界での防御の一部であるデバイスで使用される場合は、セキュリティ上の問題を引き起こす可能性があります。 また、標準への準拠という観点からは要求されていても、セキュリティの観点では必ずしも望ましくないデフォルト設定もあります。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

パスワード管理

簡易ネットワーク管理プロトコル（SNMP）のコミュニティ ストリングなど、パスワードと同様

の機能情報は、CSS への不正アクセスに対する主要な防御手段です。 大半のパスワードを扱う最善の方法は、TACACS+ または RADIUS 認証サーバ上に保持するというものです。 ただし、ほとんどの CSS には依然として、特権アクセス用にローカルで設定されたパスワードがあります。 また、CSS では、その他のパスワード情報をコンフィギュレーション ファイルに含めることができます。 クリア テキストで設定されたパスワードはいずれも、データ暗号規格（DES）で暗号化された設定に表示されます。

ローカル ユーザのプロファイル

このリストには、ローカル ユーザのプロファイルが記述されます。

- *Administrator* : [Administrator] プロファイルには、次の 3 つの特権が含まれます。[Offline Diagnostics Monitor] メニューへのアクセスコマンドラインへのフル アクセスフル ディレクトリ アクセスこれらの設定は、コマンドラインまたは [Offline Diagnostics Monitor] メニューから設定できます。
- *Technician* : [Technician] プロファイルには、次の権限が含まれます。コマンドラインへのフル アクセスフル ディレクトリ アクセスこれらの設定は、コマンドラインを使用して設定できます。 [Technician] プロファイルは、CSS の管理には使用しないでください。
- *Superuser* : [Superuser] のプロファイルには、次の権限が含まれます。コマンドラインへのフル アクセスディレクトリ アクセスの制限を保存する能力これらの設定は、コマンドラインを使用して設定できます。
- *User* : [User] プロファイルは、設定に変更を加えることができません。また、ディレクトリ アクセスの制限が含まれます。 これらの設定は、コマンドラインを使用して設定できます。

restrict user-database コマンドを実行すると、各ユーザにディレクトリ アクセスの制限が適用されます。 Administrator および Technician のユーザ レベルだけが、次の操作を実行できます。

- **restrict user-database** コマンドを削除します。
- **local user-database** コマンドを変更します。
- **clear running-config** コマンドを実行します。

インタラクティブ アクセスの制御

CSS にログインできるユーザは、一般大衆が必ずしも確認する必要のない情報を表示できます。場合によっては、CSS にログインできるユーザは、ネットワーク攻撃のリレーとして CSS を使用できます。 CSS への特権アクセスを行うユーザは CSS を再設定できます。 不適切なアクセスを防ぐために、CSS へのインタラクティブ ログインを制御する必要があります。

ほとんどのインタラクティブ アクセスはデフォルトで無効になっていますが、例外があります。最も明らかな例外は、コンソール端末など、直接接続した非同期端末からのインタラクティブ セッションと、イーサネット管理ポートへのアクセスです。

CSS へのインタラクティブ アクセスの制御方法の詳細については、「CSS リモート アクセス方式の設定」を参照してください。

コンソール ポート

重要な項目は、シスコ デバイスのコンソール ポートには特別な権限があることです。 特に、POST 診断の実行時に、ユーザが ESC（エスケープ）文字をコンソール ポートに送信したと想定します。 リブート後に、このユーザは、簡単にパスワード回復手順を実行してシステムを制御

することができます。 電源を切断したり、システム クラッシュを引き起こしたりできる攻撃者や、直結配線された端末、モデム、ターミナル サーバ、またはそれ以外のネットワーク デバイス経由でコンソール ポートにアクセスできる攻撃者は、システムを制御できます。 これらの攻撃者は、システムに物理的にアクセスできない場合や、正常にログインできない場合でも、システムを制御できます。

したがって、シスコ コンソール ポートにアクセスするネットワーク デバイスやモデムは、CSS への特権アクセスに使用されるセキュリティと同等での標準に適合するように保護する必要があります。 少なくとも、コンソール モデムには、ダイヤルアップ ユーザがアクセスする際にパスワードを要求するタイプのものを使用し、モデム パスワードの管理に注意を払うことが必要です。

一般的なインタラクティブ アクセス

CSS へのインタラクティブ接続を確立する方法は、ユーザが認識しているより数多くあります。 CSS を管理するには、次の方式を使用できます。

- Telnet
- Secure Shell Host（SSH）
- SNMP
- コンソール
- FTP
- XML
- Web 管理

有効または無効にするには、**restrict** コマンドを実行します。 CSS は、特定のポートでの受信を続行しますが、接続は閉じられます。 パケットがこれらのポートで受信されないように、アクセス コントロール リスト（ACL）の句を設定してパケットを拒否してください。

考えられるアクセス モードがすべてブロックされていることを確認するのは困難です。 ほとんどの場合、管理者は、すべての回線でのログインが確実に制御されているようにするために、なんらかの認証メカニズムを使用する必要があります。 管理者は、信頼できないネットワークからはアクセスできないマシンでも、ログインが制御されているようにする必要があります。

コンソール アクセスの制御

デフォルトでは、コンソールは、ローカルに設定されたユーザ プロファイルを使用して認証します。 TACACS+ または RADIUS 認証をアクティブにするには、**console authentication** グローバル コマンドを関連オプションとともに実行します。

VTY の制御

デフォルトでは、vtys は、ローカルに設定されたユーザ プロファイルを使用して認証します。 TACACS+ または RADIUS 認証をアクティブにするには、**virtual authentication** グローバル コマンドを関連オプションとともに実行します。

SSH サポート

SSH などの暗号化されたアクセス プロトコルがソフトウェアでサポートされている場合は、SSH サーバの使用時にそのプロトコルだけを有効にし、Telnet アクセスを無効にすることを推奨します。 SSH デーモン（SSHD）を有効にするには、SSHD サーバのライセンスが必要です。こ

のライセンスで、CSS ソフトウェアの標準および拡張の両バージョンの SSHD 機能が有効になります。 **sshd** コマンドを実行します。 詳細については、「CSS ネットワーク プロトコルの設定」を参照してください。

注: SSH バージョン 1 のサポートは 4.01 で開始されました。 SSH バージョン 2 のサポートは 5.20 で開始されました。

RADIUS

バージョン 5.00 以降では、ユーザ認証に RADIUS を使用するように CSS を設定できます。 RADIUS 認証を行うように CSS を設定するには、「ユーザ プロファイルおよび CSS パラメータの設定」を参照してください。

注: ユーザまたはグループのプロファイルに必要なのは、インターネット技術特別調査委員会（ IETF ）RADIUS 属性、[006] Service-Type = administrative だけです。

次のリストは、デバッグ メッセージ コードを示します。

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

RADIUS ログインに関連付けられたデバッグを表示するには、次のコマンドを実行します。

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

次に示すのは、正常な認証のデバッグ例です。

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

次に示すのは、ユーザ名またはパスワードが誤っているために失敗した認証の例です。

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

次に示すのは、ユーザ プロファイルの RADIUS 属性 006 service-type が設定されていないために失敗した認証の例です。

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

TACACS+

バージョン 5.03 以降では、ユーザ認証に TACACS+ を使用するように CSS を設定できます。 TACACS+ 認証を行うように CSS を設定するには、Cisco CSS 11000 シリーズのリリース ノートを参照してください。

TACACS+ ログインに関連付けられたデバッグを表示するには、次のコマンドを実行します。

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

次に示すのは、正常な認証のデバッグ例です。

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

次に示すのは、ユーザ名またはパスワードが誤っているために失敗した認証の例です。

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

警告バナー

司法管轄区域によっては、権限のないユーザに、無許可で使用していることを伝えるバナーを表示していると、システムに侵入したクラッカーに対する民事および刑事訴訟の手続きが大幅に軽減される場合があります。 また、ユーザに意図を通知する手順を踏んでいない限り、不正ユーザのアクティビティに対しても監視を禁じている管轄区域もあります。 この通知を表示する方法の 1 つが、バナー メッセージの表示です。 バナー メッセージは、CSS の **set banner** コマンドで設定できます。 このコマンドは 5.03 で導入されました。

法的通知要件は複雑で、管轄区域や状況によってさまざまです。 同じ管区地域内でも、法的見解が異なります。 この問題については、担当の弁護士と協議してください。 弁護士と協力して、次の通知のどれをバナーに含めるかを検討してください。

- システムにログインしたり、システムを使用したりできるのは、特別に承認された人のみであることを明示し、場合によっては、使用を承認できる担当者の情報を含む通知。
- システムの不正な使用は違法であり、民事罰または刑事罰が課される場合があることを伝える通知。
- システムのすべての使用は、これ以上の警告なしに記録または監視され、その結果、得られたログが裁判所で証拠として使用される場合があることを伝える通知。
- 地域の法律で要求される特定の通知。

（法的ではなく）セキュリティ上の理由から、CSS に関する次の情報はログイン バナーに含めないでください。

- 名前
- モデル
- 動作するソフトウェア
- 主催者（Owner）

一般に設定されている管理サービス

多くのユーザは、インタラクティブ リモート ログイン以外のプロトコルを使用して、自身のネットワークを管理しています。 この目的で最もよく使用されるプロトコルは SNMP と HTTP です。 最も安全な選択肢は、これらのプロトコルをすべて、有効にしないことです。 しかし、プロトコルのいずれかを有効にした場合は、この項の説明に従って保護してください。

SNMP

SNMP は、ネットワーク デバイスの監視と、多くの場合、設定の変更に非常に広く使用されています。 SNMP には 2 種類の主要な標準バージョン、SNMPv1 および SNMPv2 があります。 CSS は、コミュニティ ベースの SNMP として知られる SNMP バージョン 2C（SNMPv2C）をサポートしています。 CSS は、SNMPv1 形式のトラップを生成します。

CSS への SNMP アクセスを制御するには、**no restrict snmp** コマンドと **restrict snmp** コマンドを実行します。 SNMP によるアクセスはデフォルトで有効になっています。 SNMP によるアクセスを無効にした場合でも、CSS は引き続き、特定のポート 1 で受信しますが、接続は閉じられます。 パケットを拒否する ACL 句を設定し、パケットが SNMP のポートで受信されないようにします。

残念ながら、SNMPv1 および SNMPv2c では、コミュニティ ストリングに基づく非常に脆弱な認証方式を使用します。 認証では、暗号化されずにネットワーク経由で送信される固定パスワードが使用されることになります。 SNMPv2C を使用する必要がある場合は、あいまいなコミュニティ ストリングを選択するよう注意してください（そして、public や private などを使用しないでください）。 可能な場合は、すべてのネットワーク デバイスで同じコミュニティ ストリングを使用しないようにしてください。 デバイスごと、少なくともネットワークのエリアごとに異なるストリングを使用してください。 また、読み取り専用ストリングと読み書き用ストリングを同じものにしないでください。 可能であれば、読み取り専用のコミュニティ ストリングで定期的な SNMPv2C ポーリングを実行します。 読み取り/書き込みストリングは、実際の書き込み処理のみに使用してください。

SNMPv2C は、次の理由により、公衆インターネット上での使用には適していません。

- SNMPv2C では、クリア テキストの認証文字列が使用される。
- SNMPv2C は、簡単にスプーフィングされるデータグラム ベースのトランザクション プロトコルである。
- ほとんどの SNMP 実装で、定期ポーリングの一環としてクリアテキストの認証ストリングが何度も送信される。

公衆インターネット上で SNMPv2C を使用する場合は、これらの影響を慎重に考慮してください。

ほとんどのネットワークにおいて、正規の SNMP メッセージは特定の管理ステーションからのみ発信されます。 正規の SNMP メッセージがネットワーク内の特定の管理ステーションからのみ発信される場合は、不要な SNMP のメッセージを拒否するために、回線 VLAN に適用される ACL の使用を検討してください。

SNMP 管理ステーションには、多くの場合、コミュニティ ストリングなどの認証情報を含む大規模なデータベースが存在します。 この情報により、多数の CSS やその他のネットワーク デバイスへのアクセスが可能になります。 このように情報が集中しているため、SNMP 管理ステーションは、必然的に攻撃の的となります。 それに備えて、SNMP 管理ステーションは厳重に保護してください。

HTTP

CSS は、Extensible Markup Language（XML）文書を使用する HTTP プロトコルを介したリモート設定をサポートしています。 WebNS バージョン 4.10 以前では、TCP ポート 8081 を参照すると、WebNS デバイス管理ユーザ インターフェイスにクリア テキストでアクセスできます。 一般に HTTP アクセスは、CSS へのインタラクティブ アクセスと同等です。 HTTP に使用される認証プロトコルは、ネットワークでクリア テキストのパスワードを送信することと同等です。 残念ながら HTTP には、確認要求ベースや 1 回限りのパスワードを使用する有効な方法がありません。 したがって、HTTP は、公衆インターネット上で使用するには比較的な危険な選択肢です。

管理に HTTP を使用することを選択した場合は、回線 VLAN に適用される ACL を使用して、適切な IP アドレスへのアクセスを制限してください。 CSS への HTTP XML アクセスを制御するには、**no restrict xml** コマンドと **restrict xml** コマンドを実行します。 より新しい WebNS のバージョンでは、コマンドが **web-mgt state [disable / enable]** に変更されています。 HTTP XML によるアクセスはデフォルトで無効になっています。 CSS への HTTP WebNS デバイス管理ユーザ アクセスを制御するには、**no restrict web-mgmt** コマンドと **restrict web-mgmt** コマンドを実行します。 WebNS デバイス管理ユーザ インターフェイスは、デフォルトで無効になっています。 ポート 8081 の CSS を参照するには、**no restrict xml** コマンドと **no restrict web-mgmt** コマンドの両方を実行する必要があります。

バージョン 5.00 以降では、ポート 8081 の回線アドレスを HTTP で参照すると、HTTPS を使用するようにブラウザがリダイレクトされ、同じ回線アドレスに接続します。

HTTPS

CSS は、HTTP Secure (HTTPS) プロトコルを介したリモート設定をサポートしています。 この Secure Socket Layer (SSL) により、WebNS デバイス管理ユーザ インターフェイスと Web ブラウザ間のデータ転送 (パスワードを含めることができる) が保護されます。

CSS への HTTPS WebNS デバイス管理ユーザ アクセスを制御するには、**no restrict web-mgmt** コマンドと **restrict web-mgmt** コマンドを実行します。 WebNS デバイス管理ユーザ インターフェイスは、デフォルトで無効になっています。 これが無効になっている場合、CSS は特定のポートで受信を続行しますが、接続は閉じられます。 パケットが SSL TCP ポート 443 で受信されないように、ACL の句を設定してパケットを拒否してください。

インターネット (およびその他の信頼できないネットワーク) による管理およびインタラクティブ アクセス

多くのユーザはこれらの CSS をリモートで管理しており、ときにはインターネット上で管理されます。 暗号化されていないリモート アクセスはリスクを伴いますが、インターネットのような公衆ネットワーク経由のアクセスは特に危険です。 インタラクティブ アクセス、HTTP、SNMP などのリモート管理方式にはいずれも脆弱性があります。

この項で説明する攻撃はかなり複雑なものですが、今日のクラッカーにとって、決して実行できないものではありません。 適切なセキュリティ対策を講じている公衆ネットワーク プロバイダーは、多くの場合、これらの攻撃者を阻止できます。 管理トラフィックを伝送するすべてのプロバイダーが使用するセキュリティ対策の信頼度を評価します。 プロバイダーを信頼している場合でも、少なくとも、これらのプロバイダーの不備の結果から自らを守る対策を講じてください。

この項の注意事項は、CSS と同様にホストにも適用されます。 このドキュメントでは、CSS ログイン セッションを保護する方法を説明しますが、ホストをリモートで管理している場合に、同様のメカニズムを使用してホストを保護する方法も説明します。 リモート インターネット管理は便利ですが、セキュリティに対する十分な注意が必要です。

パケット スニファ

クラッカーは、インターネット サービス プロバイダーが所有するコンピュータ、または他の大規模ネットワーク上のコンピュータに頻繁に侵入します。 クラッカーはパケット スニファ プログラムをインストールし、ネットワークを通過するトラフィックを監視します。 これらのパケット

スニファ プログラムは、パスワードや SNMP コミュニティ ストリングなどのデータを盗みます。 ネットワーク オペレータはセキュリティの改善を開始しているため、この攻撃はより困難になっています。 しかし、依然としてこの攻撃は、比較的よく見られます。 外部のクラッカーによるリスクの他に、不正なインターネット サービス プロバイダー従業員がスニファをインストールする場合もあります。 非暗号化チャネルを経由して送信されるパスワードは危険にさらされます。これには、CSS のログインおよび有効化パスワードが含まれます。

できれば、信頼できないネットワーク上で非暗号化プロトコルを使用して CSS にログインすることは避けてください。 CSS ソフトウェアがサポートする場合は、SSH などの暗号化ログイン プロトコルを使用します。

暗号化されたリモート アクセス プロトコルにアクセスできない場合は、CSS へのインタラクティブ ログインと特権アクセスの両方を制御するために、S/KEY や OPIE などの 1 回限りのパスワード システムを、TACACS+ または RADIUS サーバとともに使用するという方法もあります。 利点は、盗まれたパスワードは機能しないことです。 盗まれたパスワードは、それが盗まれたセッション自体によって無効になります。 セッションで送信され、パスワードとの関連のないデータは、クラッカーが利用可能なままですが、スニファ プログラムの多くはパスワードに集中するように設定されています。

クリア テキスト Telnet セッションでパスワードを送信する必要がある場合は、パスワードを頻繁に変更してください。 そして、セッションが経由するパスには細心の注意を払ってください。

インターネット アクセスに関するその他の危険性

パケット スニファの他にも、CSS のリモート インターネット管理には次のようなセキュリティ リスクがあります。

- インターネット経由でルータを管理するには、少なくとも数台のインターネット ホストに CSS へのアクセスを許可する必要があります。 これらのホストが攻撃されることも、そのアドレスがスプーフィングされることもあります。 インターネットからのインタラクティブ アクセスを許可した場合、セキュリティは、自分のスプーフィング対策だけでなく、関係するサービス プロバイダーのスプーフィング対策にも依存します。次の手順を実行すると、これらの危険を軽減できます。CSS へのログインが許可されたすべてのホストが、自分の管理下にあることを確認します。強力な認証機能を備えた暗号化ログイン プロトコルを使用します。
- 暗号化されていない TCP の接続（Telnet セッションなど）へのアクセスが入手可能な場合もあります。 このタイプのセッションにアクセスできるユーザは、ログインしているユーザから制御を事実上、奪うことができます。 このような攻撃は、単純なパケット スニフィングほど一般的ではなく、実行方法も複雑であると考えられます。 しかし、このような攻撃は可能であり、特定のネットワークをターゲットとして狙っている攻撃者は、これを実行できます。 セッション ハイジャックの問題に対する唯一の現実的な対策は、強力な認証機能を備えた暗号化管理プロトコルを使用することです。
- インターネット上では、サービス拒否（DoS）攻撃が比較的よく見られます。 ネットワークが DoS 攻撃を受けている場合は、CSS にアクセスして情報を収集したり、防御措置を講じたりできない可能性があります。 他者のネットワークへの攻撃によって、自分のネットワークへの管理アクセスが影響されることさえあります。 DoS 攻撃に対するネットワークの抵抗力を高めるために対策を講じることは可能ですが、このリスクに対する現実的な防御策は、緊急時に使用するための別系統の帯域外管理チャネル（ダイヤルアップ モデムなど）を用意しておくこと以外にありません。

ロギング

シスコ CSS では、各種のイベントに関する情報を記録できますが、これらの多くにはセキュリティ上、重要な情報が含まれています。 ログは、セキュリティ事象への特性化および応答に非常に役立ちます。 **logging subsystem** コマンドを実行すると、CSS でログを有効にすることができます。 デフォルトのログ レベルは、すべてのサブシステムで warning-4 です。

この情報を収集するには、サブシステムのロギング用の次のコマンドを実行します。

- ユーザ ログイン
- ログアウト
- RADIUS 認証
- TACACS+ 認証

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

注: netman subsystem コマンドで、TACACS+ をデバッグできます。

セキュリティの観点からは、システム ログに通常記録される最も重要なイベントは次のイベントです。

- インターフェイス ステータスの変化
- システム設定の変更
- ACL の一致

```
logging subsystem netman level info-6
!--- Note that the default logging level is warning-4, which does !--- not appear in the
configuration. logging commands enable
logging subsystem acl level debug-7
```

リモート モニタリング（RMON）を使用すると、CSS イーサネット ポートのパケットのアクティビティをリモートで監視および分析できます。 また、RMON では、MIB オブジェクト監視のアラームを設定したり、イベントを設定してこれらのアラーム状態を通知したりできます。 RMON イベントは、関連付けられた RMON アラームがトリガーされたときに発生する動作です。 アラーム イベントは、その発生時に、次の項目のいずれかまたは両方を生成するようにを設定できます。

- ログ イベント
- SNMP ネットワーク管理ステーションへのトラップ

ログ情報の保存

デフォルトでは、CSS により、ハード ディスクまたはフラッシュ ディスクでログ ファイルに、ブートおよびサブシステム イベント ログ メッセージが保存されます。 これらのファイルの内容は ASCII テキストで記録されます。 また、アクティブな CSS セッション、電子メール、別のホスト システムにログ メッセージを送信するように CSS を設定することもできます。

ローカル ログ ファイルの最大サイズは、ハード ディスク ベース システムでは 50 MB、フラッシュ ディスク ベースのシステムでは 10 MB です。

サブシステム ログ メッセージは、CSS の動作中に発生するサブシステム イベントです。 CSS は、これらのメッセージを sys.log ファイルに保存します。 CSS は、ログに記録する必要がある最初のサブシステム イベントが発生すると、このファイルを作成します。 CSS は、記録するサブシステム メッセージを、設定されているログ レベルで決定します。

大規模なインストレーションには、ほとんどの場合 syslog サーバがあります。 **logging host** コマンドを実行すると、ホスト システムの syslog デーモンにログ情報を送信できます。 Syslog サーバがある場合でも、ディスクに対してローカル ロギングを有効にする必要があります。

すべてのログには、月、日、および秒までの時間のタイムスタンプが付けられます。 Simple Network Time Protocol (SNTP) などの一般的な時刻ソースをログに設定すると、記録されたイベントのシーケンスを、より簡単に追跡できます。 CSS で SNTP サーバを設定するには、**sntp** コマンドを実行します。 SNTP は 5.00 コードで導入されました。

アクセス リスト違反の記録

回線アドレスまたはコンテンツ ルールの仮想 IP (VIP) アドレスにアクセスするトラフィックを、ACL を使用してフィルタリングする場合は、フィルタ基準に違反したパケットをロギングすることもできます。 ACL 句でロギングを有効にするには、**clause # log enable** コマンドを実行します。 また、**logging subsystem acl level debug-7** コマンドを実行します。 CSS は次の情報を記録します。

- プロトコル
- 送信元ポート
- 宛先ポート
- ソース IP アドレス
- 宛先 IP アドレス

大量のパケットに一致する ACL エントリのロギングを設定しないようにしてください。 このような設定により、ログ ファイルのサイズが極端に大きくなり、システムのパフォーマンスが低下する可能性があります。

また、ACL ロギングを使用して、ネットワーク攻撃に関連付けられたトラフィックを識別することもできます。 この場合は、疑わしいトラフィックを記録するように ACL ロギングを設定します。 ACL を作成するために、CSS のインターネット側のシスコ ルータで識別することができます。 詳細については、「シスコ ルータを使用したパケット フラッドの識別とトレース」を参照してください。

注: CSS ACL は着信パケットだけに適用されます。 ACL では、インターフェイスからの発信パケットは検査されません。

IP ルーティングの保護

この項では、ルータによる IP パケットの転送方法に関連する基本的なセキュリティ対策について説明します。 これらの問題に関する詳細については、「Cisco ISP Essentials - すべての ISP が必ず考慮すべき重要な IOS 機能」を参照してください。

デフォルトでは、CSS は次のように設定されます。

- CSS が DoS 攻撃としてログに記録する前に VIP に転送される SYN パケットの数を制限する
  注: この動作を無効にすることはできません。

- ダイレクト ブロードキャストを拒否する
- 送信元と宛先の IP アドレスが同じであるパケットを拒否する
- マルチキャスト送信元の IP アドレスを拒否する
- 送信元または宛先のポートが 0 のパケットを拒否する

スプーフィング対策

ネットワーク攻撃の多くは、攻撃者による IP データグラムの送信元アドレスの偽装、つまりスプーフィングによって行われます。 攻撃によっては、スプーフィングに依存して攻撃が実行されます。 また、攻撃者が自分自身のではなく、他者のアドレスを使用できる場合はトレースが非常に困難になる攻撃もあります。 したがって、実行可能な場合は必ずスプーフィングを防止することは、ネットワーク管理者にとって重要です。

スプーフィング対策は、現実的な場合は必ず、ネットワークでのすべてのポイントで行う必要があります。 ただし、スプーフィング対策は通常、大規模なアドレス ブロック間またはネットワーク管理のドメイン間の境界で最も容易かつ有効です。 どの送信元アドレスが特定のインターフェイスで正規に表示できるかを決定するのは困難であるため、ネットワーク内のルータのスプーフィング対策は通常、実際的ではありません。

インターネット サービス プロバイダー (ISP) である場合は、効果的なスプーフィング対策を他の効果的なセキュリティ対策とともに講じると、サブスクライバが他のプロバイダーに移行してしまうという重大な問題が発生する可能性もあります。 ISP である場合は、ダイヤルアップ プールやその他のエンド ユーザ接続ポイントにスプーフィング対策の制御を適用するように特に注意してください。

注: RFC 2267 を参照してください。

企業のファイアウォールや境界ルータの管理者は、インターネット上のホストが内部ホストのアドレスを使用できないようにスプーフィング対策手段をインストールすることもあります。 ただし、この場合でも、内部ホストはインターネット上のホストのアドレスを使用できます。 両方向のスプーフィングを防止するようにしてください。 組織のファイアウォールで両方向のスプーフィング対策をインストールすることには、少なくとも次の 3 つの正当な理由があります。

- 内部ユーザがネットワーク攻撃を仕掛けようという気を起こさなくなり、攻撃を試みたとしても成功する可能性が低くなります。
- 不注意で誤って設定された内部ホストが、リモート サイトでの問題を引き起す可能性が低くなります。 したがって、お客様が不満を感じる可能性も低くなります。
- 外部クラッカーは、さらなる攻撃の開始点として、しばしばネットワークに侵入してきます。 このようなクラッカーは、発信スプーフィング保護付きのネットワークにはそれほど興味を持ちません。

ACL によるスプーフィング対策

残念ながら、適切なスプーフィング保護を提供するコマンドを単に一覧表示することは、実用的ではありません。 ACL 設定は、個々のネットワークによって大きく異なります。 基本的な目標は、あらかじめ想定された送信元アドレスから経由可能なパス以外のインターフェイスにパケットが到達した場合に、そのパケットを廃棄することです。 たとえば、サーバ ファームをインターネットに接続する 2 回線 CSS で、インターネット回線に到達したデータグラムのうち、その送信元アドレス フィールドではサーバ ファームのマシンから発信されたことになっているものを廃棄するとします。

同様に、サーバ ファームに接続されているインターフェイスに到達したデータグラムのうち、その送信元アドレス フィールドではサーバ ファームの外部にあるマシンから発信されたことになっているものも廃棄します。 CPU のリソースで可能な場合は、どのトラフィックが正規に到達できるかの判断が可能なすべての回線にスプーフィング対策を適用します。

トランジット トラフィックを伝送している ISP では、スプーフィング対策 ACL を設定できる機会が限られますが、このような ISP では通常、その ISP のアドレス レンジ内で発信されたことになっている外部トラフィックをフィルタリングできます。

一般に、スプーフィング対策フィルタは、入力 ACL で構築する必要があります。 パケットは、到着する回線でフィルタリングされる必要があります。 CSS は、着信パケットだけに ACL を適用できます。

スプーフィング対策 ACL がある場合は、ブロードキャストまたはマルチキャストの送信元アドレスを持つデータグラムを常に拒否する必要があります。 デフォルトで、CSS はこれらのデータグラムを拒否します。 スプーフィング対策 ACL は、予約ループバック アドレスが送信元アドレスであるデータグラムを拒否する必要があります。 また、通常、送信元と宛先のアドレスに関係なく、すべてのインターネット制御メッセージ プロトコル (ICMP) リダイレクトをスプーフィング対策 ACL がフィルタリングで拒否するようにする必要があります。 CSS ACL では、ICMP タイプを拒否するように指定することはできません。 その代わり、**no redirects** コマンドを実行して、すべての回線 IP アドレスで ICMP リダイレクトを受け入れないように設定します。 そのコマンドは次のとおりです。

```
clause # deny any 127.0.0.0 255.0.0.0 destination any
clause # deny any 0.0.0.0 0.0.0.0 destination any
```

注: clause # deny any 0.0.0.0 0.0.0.0 destination any コマンドで、多くのブートストラップ プロトコル (BOOTP) /DHCP クライアントからのパケットがフィルタリングにより拒否されます。したがって、このコマンドはすべての環境に適しているわけではありません。

ダイレクト ブロードキャストの制御

非常によく見られる SMURF DoS 攻撃とその関連の攻撃では、IP ダイレクト ブロードキャストが使用されます。 デフォルトでは、CSS が **no ip subnet-broadcast** コマンドで設定されており、ダイレクト ブロードキャストは拒否されます。

IP ダイレクト ブロードキャストとは、送信元のマシンが直接接続されていないサブネットのブロードキャスト アドレスに送信されるデータグラムです。 ダイレクト ブロードキャストは、ターゲット サブネットに到達するまでユニキャスト パケットとしてネットワーク経由でルーティングされます。 サブネットで、ダイレクト ブロードキャストは、リンク層ブロードキャストに変換されます。 IP アドレス設定アーキテクチャの性質により、最終的にダイレクト ブロードキャストを識別できるのは、チェーンの最後のルータまたはレイヤ 3 ネットワーク デバイスのみです。このデバイスは、ターゲット サブネットに直接接続されています。 ダイレクト ブロードキャストは、正当な目的のために使用される場合もありますが、そのような使用方法は金融サービス業界以外では一般的ではありません。

SMURF 攻撃では、攻撃者は偽装した送信元アドレスからダイレクト ブロードキャスト アドレスに ICMP エコー要求を送信します。 その結果、ターゲット サブネットのすべてのホストは、偽装した送信元に応答を送信します。 攻撃者は、このような要求の継続的なストリームを送信すると、非常に大きな応答のストリームを作成できるようになるため、アドレスが偽装されたホストが完全に満杯状態になる場合があります。

一部のファイアウォール ルータ (ネットワーク設計に依存する) の SMURF 攻撃をブロックする

戦略については、「The Latest in Denial of Service Attacks: ""Smurfing" Description and Information to Minimize Effects」を参照してください。 この文書には、SMURF 攻撃に関する一般情報も含まれています。

パスの完全性

多くの攻撃は、ネットワーク内でデータグラムが経由するパスを操作する能力に依存しています。 クラッカーがルーティングを制御している場合は、他のユーザのマシンのアドレスをスプーフィングして、リターン トラフィックを自分宛てを送信させることができる場合があります。 場合によっては、クラッカーが他者宛てのデータを代わりに受信して読み取ることができます。 ルーティングも、純粋に DoS の目的で中断できます。

IP ソース ルーティング

IP プロトコルはソース ルーティング オプションをサポートします。このオプションを使用すると、IP データグラムの送信者が、最終的な宛先に到達するまでにデータグラムがたどる経路を制御でき、通常は、その返信がたどる経路も制御できます。 これらのオプションが実際のネットワークで正規の目的のために使用されることはまれです。 より古い IP 実装の中には、ソースルート パケットを正しく処理しないものもあります。 ソース ルーティング オプションを指定してデータグラムを送信できますが、その結果、これらの実装を実行しているマシンがクラッシュする場合があります。

CSS は通常、**no ip source-route set** コマンドで設定されています。 CSS は、ソース ルーティング オプションを含む IP パケットを転送することはありません。 ネットワークでソース ルーティングが必要なことがわかっている場合を除き、デフォルト マンドを設定したままにしてください。

ICMP リダイレクト

ICMP リダイレクト メッセージは、エンド ノードに対して、特定の宛先へのパスとして特定のルータを使用するように指示します。 正常に機能している IP ネットワークでは、ルータは、ルータのローカル サブネット上のホストにのみリダイレクトを送信します。 エンド ノードがリダイレクトを送信することも、リダイレクトが複数のネットワーク ホップを通過することもありません。 ただし、攻撃者はこれらのルールに違反することができ、一部の攻撃はこれらのルールに基づいています。 管理ドメイン間の境界に位置するすべてのルータの入力インターフェイスで受信方向の ICMP リダイレクトを遮断してください。 さらに、シスコ ルータ インターフェイスの入力側に ACL を適用し、すべての ICMP リダイレクトを遮断することができます。 このフィルタリングにより、正しく設定されているネットワークに運用上の影響が生じることはありません。

このタイプのフィルタリングは、リモート攻撃者によるリダイレクト攻撃だけを阻止します。 さらに、攻撃者のホストが攻撃対象のホストと同じセグメントに直接接続されている場合、攻撃者は、リダイレクトを使用して重大な問題を引き起こすことができます。

デフォルトでは、CSS が、設定された各回線 IP アドレスでリダイレクトを受け入れるように設定されています。 この機能をオフにするには、回線 IP アドレスで **no redirect** コマンドを実行します。

ルーティング プロトコルのフィルタリングと認証

認証をサポートしているダイナミック ルーティング プロトコルを使用する場合は、認証機能を有効にします。 認証は、ルーティング インフラストラクチャへの悪意のある攻撃を阻止するととも

に、ネットワーク上にある、不適切な設定の不正なデバイスが引き起こす可能性がある損害を防ぐのに役立ちます。

同じ理由で、大規模なネットワークのサービス プロバイダーおよび他のオペレータは、ルート フィルタリングの使用を検討できます。 ルート フィルタリングでは、ネットワーク ルータで、明らかに不正なルーティング情報が受け入れられません。 ルート フィルタリングを実行するには、コマンドで **distribute-list** パラメータを使用します。 経路フィルタリングを過剰に使用すると、ダイナミック ルーティングの利点がなくなる場合があります。 ただし、選択的に使用すると、多くの場合、不都合な結果を回避できます。 たとえば、スタブ カスタマー ネットワークと通信するためにダイナミック ルーティング プロトコルを使用する場合は、お客様に実際に委譲したアドレス レンジへのルートを除き、お客様からのルートを受け入れないでください。

CSS はルートをフィルタリングすることはできません。 代わりに、この機能で CSS のルーティング ピアを設定します。

この文書には、ルーティング認証とルート フィルタリングの設定に関する詳細な指示は含まれていません。 このようなドキュメントは、Cisco.com やその他のサイトで入手できます。 ドキュメント「Cisco ISP Essentials - すべての ISP が必ず考慮すべき重要な IOS 機能」を参照してください。 設定手順は複雑であるため、初心者である場合は、重要なネットワークでこれらの機能を設定する前に経験者のアドバイスを受けてください。

フラッド管理

Dos 攻撃の多くでは、無用なパケットのフラッドが多用されます。 これらのフラッドによってネットワーク リンクが過密状態になり、ホストの処理速度が低下して、さらにルータが過負荷状態になります。 このようなフラッドによる影響は、ルータを注意深く設定することで軽減できます。

フラッド管理の重要な部分は、パフォーマンスのボトルネックが生じる可能性がある場所を認識することです。 フラッドで T1 回線が過負荷になる場合は、回線のソース側のルータでフラッドを遮断してください。 この場合、宛先側で遮断しても、効果はほとんどありません。 ルータ自体が最も過負荷になるネットワーク コンポーネントである場合は、ルータに大きな負荷がかかる保護をフィルタリングすると、事態が悪化する可能性があります。 この項に記載されている提案の実装を検討する際は、この点に留意してください。

トランジット フラッド

アップストリームの Cisco IOS® ルータで Cisco QoS 機能を使用して、ある種のフラッドから CSS、ホスト、リンクを保護することができます。 残念ながら、このドキュメントでは、この種のフラッド管理の一般的な手順は説明していません。 また、保護方法は、攻撃方法に応じて大幅に異なります。 単純で一般的に適用可能な唯一のアドバイスは、CPU リソースがサポートしている場合は必ず、Weighted Fair Queueing (WFQ; 重み付け均等化キューイング) を使用するということです。 WFQ は、Cisco IOS ソフトウェアの最近のバージョンで、低速シリアル回線向けのデフォルトになっています。 考えられるその他の機能は次のとおりです。

- 専用アクセス レート (CAR)
- ジェネリック トラフィック シェーピング (GTS)
- カスタム キューイング

場合によっては、アクティブな攻撃の下でこれらの機能を設定できます。

CSS は、VIP および実サーバへの SYN フラッド攻撃の影響を軽減できます。 デフォルトで CSS

は、SYN および不完全な 3 方向ハンドシェイクの数を制限し、それらを DoS 攻撃として ログに記録します。

詳細については、「セキュリティ リファレンス情報」を参照してください。

不要な可能性のあるサービス

一般的なルールとして、潜在的に悪意のあるネットワークから到達可能なルータでは、不要なサービスを無効にしてください。 この項に記載されたサービスは、有用である場合があります。 ただし、アクティブに使用されていない場合は、これらのサービスを無効にしてください。

SNTP

SNTP は特に危険ではありませんが、不要なサービスは侵入経路となる可能性があります。 実際に SNTP を使用している場合は、信頼できる時刻ソースを明示的に設定してください。 SNTP では認証を使用しません。 時間ベースの破壊は、特定のセキュリティ プロトコルを無力化する効果的な方法です。 最善の方法は、スプーフィングされる可能性の低い内部のソースを使用することです。

Cisco 発見プロトコル

WebNS 5.10 で導入された Cisco Discovery Protocol (CDP) は、一部のネットワーク管理機能に使用されます。 CDP は、直接接続されたセグメントのどのシステムでも次のアクションを実行できるため、危険です。

- ルータがシスコ デバイスであることを認識する
- モデル番号と実行中のソフトウェア バージョンを特定する

攻撃者は、この情報を使用して CSS への攻撃を設計できます。 CDP 情報は、直接接続されたシステムからのみアクセス可能です。 CSS は、CDP 情報だけをアドバタイズします。 CSS は受信しません。 **no cdp run** グローバル コンフィギュレーション コマンドを実行すると、CDP プロトコルを無効にすることができます。 インターフェイス単位で、CSS の CDP を無効にすることはできません。

最新状態の維持

他のすべてのソフトウェアと同様に、Cisco WebNS ソフトウェアにもバグがあります。 これらのバグの中には、セキュリティと密接な関係を持つものがあります。 また、新しい攻撃は絶えず開発されています。 そして、ソフトウェアの開発時には正しいと考えられていた動作は、その動作が悪用されると悪影響を及ぼす場合があります。

Cisco 製品で大きなセキュリティ上の脆弱性が新たに見つかると、通常、シスコから脆弱性に関する勧告通知が発行されます。 これらの通知が発行されるプロセスの詳細については、「セキュリティ脆弱性ポリシー」を参照してください。 通知については、「セキュリティ アドバイザリ」を参照してください。

あらゆるソフトウェアの予期しない動作は、ほとんどの場合、セキュリティ上の問題をどこかで引き起こす可能性があります。 アドバイザリには、システム セキュリティに直接影響する不具合だけが掲載されています。 セキュリティの助言がない場合でも、ソフトウェアを最新の状態に維持していれば、セキュリティを高めることができます。

セキュリティの問題には、ソフトウェアの不具合が原因ではないものもあるため、ネットワーク管理者は、攻撃の傾向を常に認識している必要があります。 これらの傾向に関心のある Web サイト、インターネット メーリング リスト、および Usenet ニュースグループは数多くあります。

関連情報

- RFC 2267
- セキュリティ アドバイザリ
- セキュリティ脆弱性ポリシー
- セキュリティに関するリファレンス情報
- CSS ネットワーク プロトコルの設定
- CSS リモート アクセス方式の設定
- ユーザ プロファイルおよび CSS パラメータの設定
- リリース ノート
- Cisco ルータを使用したパケットフラッドの識別とトレース
- Cisco ISP Essentials - すべての ISP が必ず考慮すべき重要な IOS 機能
- The Latest in Denial of Service Attacks: ""Smurfing" Description and Information to Minimize Effects
- テクニカルサポートとドキュメント - Cisco Systems